Remark

Applicant respectfully requests reconsideration of this application as amended.

No Claims have been amended. No Claims have been canceled. Therefore, claims 1-21 are now presented for examination.

Summary

Applicant's position may be summarized as follows. The present invention is unique in:

combining a decryption cipher stream and an encryption cipher stream;

using this combination to simultaneously decrypt and re-encrypt data;

applying this approach to video delivery.

Applicant respectfully submits that this is simply not shown in either reference.

35 U.S.C. §103 Rejection

Kamiya in view of Menezes

The Examiner has rejected claims 1-21 under 35 U.S.C. §103 (a) as being unpatentable over Kamiya et al., U.S. Publication No. US 2002/0106086 A1 ("Kamiya"), in view of Menezes et al., Menezes, Handbook of Applied Cryptography, ("Menezes"). This is the same rejection that was made in the previous action. The Examiner has generously provided an extensive Response to Arguments. Applicant will try to address the remaining issues in this case clearly and concisely based on the Response to Arguments.

Kamiya has been discussed extensively in prior papers and as agreed upon by both sides, it shows a decryption server 33 in Figure 1 that performs decryption and scrambling. The box is expanded in Figure 4 and, as shown there, it has a decryption unit 35A, a content decoding unit 35C, and a scramble unit 35D. The decryption unit uses a restored key combined at 35B from two keys A1 from 18, and A2 from 19 both based on A from 16 at the broadcaster. The scrambler scrambles the decoded content using a scramble key from 36.

The decoder 35C is in between the decryption unit 35A and the scramble unit 35D. Its function is described only in paragraphs 79, 80 and 104. It is an MPEG or wavelet transform decoder. This has nothing to do with decryption but instead it is about converting digital bit streams into video or audio. MPEG video is encoded primarily for compression reasons. For example, some data is converted into video by applying codewords to a look-up table, the data for some video frames is expressed as the difference from nearby frames, so the total information for such a frame can only be determined by decoding the nearby frames and applying the difference information. The decoded video is not described but is applied directly to the display (after scrambling and descrambling) so it most likely is a conventional full video signal that provides a complete (analog or digital) bitmap for each frame. The decoding process is standardized and well-documented and has nothing to do with security or encryption. It can only be performed once the data has been decrypted.

The intermediate decoding step requires that the decryption and the scrambling not be combined or performed simultaneously.

Docket No.: 42P11153   3
Application No.: 09/896,380

Menezes §§7.26 to 7.42 describes encryption and attacks with very little mention of decryption. There is no mention of decrypting with one key and encrypting with another. There is no mention of combining an encryption key with a decryption key. There is no mention of simultaneously encrypting and decrypting. In addition, there is not even any mention of combining encryption keys or simultaneously encrypting with two keys. The cascade cipher (§7.29) uses independent keys to encrypt in stages. The multiple encryption (§7.30) also uses different keys applied in different stages but the same key can be used more than once. This is further brought out in §7.40(iii) in which multiple modes may be "pipelined." Pipelining allows multiple operations to be performed quickly in series. It does not suggest simultaneous but sequential.

The Examiner refers to "CBC of multiple encryption method." Sections 7.40 and 7.41 refer to CBC. Section 7.40 refers to a composite operation of triple encryption and to sequential applications of operations. A composite operation is an operation made up of distinct parts. In other words, as in the other examples, Menezes takes different keys and applies them sequentially (one at a time) to the data. Applicant is unable to find any mention here of decrypting and re-encrypting but only encrypting and breaking the encryption.

Consider again the limitations of Claim 1. First consider, "simultaneously decrypting and re-encrypting the encrypted video." Simultaneous is occurring at the same time. In Kamiya, first the decryption happens, then the decoding happens, then the scrambling happens. In Menezes, there is no suggestion of decrypting and then re-encrypting.

Docket No.: 42P11153   4
Application No.: 09/896,380

Second consider "decrypting and re-encrypting using a combination of the first and the second cipher streams." A combination is the result of combining two things, here the first and second cipher streams. In Kamiya, the restored decryption key must be kept separate from the scrambling key so that the two operations may be performed separately. In Menezes, decryption and encryption keys are not combined. Encryption keys are not even combined except to make a third additional key in multiple encryption.

Since neither reference teaches or suggests these two limitations, Claim 1 is believed to be allowable.

The Examiner would appear be dissatisfied with the "simultaneously decrypting and re-encrypting... using a combination" expression in the claims. While Applicant does not understand this dissatisfaction, perhaps some of the dependent claims may prove to be more satisfactory.

Claim 3 recites that "the cipher stream combination comprises a result of exclusive OR-ing the first and second cipher streams." Applicant is unable to find any suggestion in either reference of exclusive OR-ing a decryption cipher stream with an encryption cipher stream.

Claim 4 recites that "the first key and the second key have symmetric agreement." Applicant is unable to find any suggestion of symmetric agreement between a decryption key and a re-encryption key.

Claim 10 recites that the encryption key is a public key and the re-encryption key is a local private key. The Examiner refers to Kamiya paragraph 21. This paragraph discusses public keys but does not mention local private keys.

Docket No.: 42P11153   5
Application No.: 09/896,380

The arguments above apply with equal force to all of the independent claims. The dependent claims are believed to be allowable therefore as well as for the limitation specifically set forth in each claim, respectively. These limitations are not specifically discussed in the interests of Examiner convenience.

Conclusion

Applicant respectfully submits that the rejections have been overcome by the amendment and remark, and that the claims as amended are now in condition for allowance. Accordingly, Applicant respectfully requests the rejections be withdrawn and the claims be allowed.

Docket No.: 42P11153   6
Application No.: 09/896,380

Invitation for a Telephone Interview

The Examiner is requested to call the undersigned at (303) 740-1980 if there

remains any issue with allowance of the case.

Request for an Extension of Time

Applicant respectfully petitions for an extension of time to respond to the

outstanding Office Action pursuant to 37 C.F.R. § 1.136(a) should one be necessary.

Please charge our Deposit Account No. 02-2666 to cover the necessary fee under 37
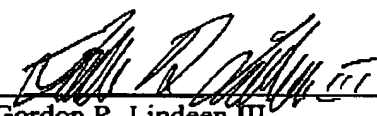
C.F.R. § 1.17(a) for such an extension.

Charge our Deposit Account

Please charge any shortage to our Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: __August 15, 2006__

Gordon R. Lindeen III
· Reg. No. 33,192

12400 Wilshire Boulevard
7th Floor
Los Angeles, California 90025-1030
(303) 740-1980